New Zealand Security Intelligence Service
Te Pā Whakamarumaru

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

11 April 2019

UNCLASSIFIED submission by Director-General of Security, NZSIS and Director General of GCSB on the Justice Committee Inquiry into the 2017 General Election and 2016 Local Elections

Director-General of Security

Thank you for inviting us to appear before you to assist with your enquiries into the 2017 General Election. We welcome this opportunity.

Before I start, I would like to acknowledge the Christchurch terrorist attacks of 15 March.

On behalf of the New Zealand Security Intelligence Service and the Government Communications Security Bureau, I would like to offer my deepest sympathies to those who have lost loved ones and to our Muslim communities.

Violent extremism has no place in New Zealand.

We welcome the Royal Commission of Inquiry. There are important questions which need answers and we embrace the opportunity to learn from this terrible experience.

NZSIS has two main priorities in relation to Christchurch. We are focused on supporting the Police investigation and the resulting prosecutions. We are also focused on mitigating the risks to New Zealanders posed by possible revenge or copycat attacks.

We are balancing these priorities against our other work – this includes our work on foreign interference – which remains absolutely vital to New Zealand's national security.

The GCSB also continues to assist NZSIS and Police in response to the Christchurch attacks.

Introductory remarks

We will lead off this morning by introducing ourselves to you and outlining our roles in relation to the protection of New Zealand's elections and democratic processes and institutions more broadly.

I am Rebecca Kitteridge and I have been the Director-General of Security at the New Zealand Security Intelligence Service since 2014.

NZSIS's role in relation to threats to elections and democratic institutions and processes is fourfold:

- First, we collect, analyse and assess intelligence about foreign interference activities in New Zealand. Our particular focus here is understanding the activities and motivations of foreign state actors operating in, or seeking to influence, New Zealand institutions, processes and individuals;

- Second, we provide intelligence to decision-makers;

- Third, we provide protective security services, advice and assistance to a wide range of individuals and entities, including Members of Parliament and Ministers; and

- Fourth, we administer the security clearance system which helps to protect New Zealand's Government against insider threat risks and espionage.

Both NZSIS and GCSB execute their functions in a way that is consistent with the provisions of the Intelligence and Security Act 2017. Importantly, NZSIS and GCSB are not law enforcement agencies and we do not make policy.

We are politically neutral public service agencies and this principle is reinforced in our governing legislation, the Intelligence and Security Act. We have a statutory obligation to brief the Leader of the Opposition on matters relating

to our functions. The Act also requires us to act independently, professionally and with integrity at all times. Our activities are guided by the National Security and Intelligence Priorities, set by Cabinet.

Director General of GCSB

I am Andrew Hampton and I am the Director-General of the Government Communications Security Bureau.

GCSB is the Government's cyber and information security authority. Our roles are also set out in the Intelligence and Security Act. In relation to foreign interference in our elections, GCSB's key roles are:

- To develop and provide intelligence (primarily foreign intelligence) and cyber assessments on the intentions, activities and capabilities of threat actors, including in relation to the Election;

- To do everything that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information infrastructures. This would include the Electoral Commission's core systems; and

- To provide cyber security and information assurance services and advice to authorised individuals and entities. This includes Members of Parliament, Ministers and other entities involved in the conduct of elections.

The Committee has requested Rebecca and I comment on how well New Zealand is positioned to protect our electoral system from foreign interference. The Committee has specifically asked us to comment on the following matters:

- The ability of foreign powers to hack the private emails of candidates or parties;

- The risk that social media based political campaigns can be made to appear as though they are domestic but are in fact created or driven by external entities; and

- The risk that donations to political parties originate from foreign governments.

Constraints on GCSB and NZSIS when talking publicly about intelligence and security matters

Before we address these issues, we would like to briefly outline the constraints we operate under when speaking publicly about our intelligence and security functions.

We are constrained in what we can say in an unclassified setting about specific foreign interference activities. This is for two main reasons:

- Firstly, we need to protect our capabilities, sources and methods. We have a longstanding practice of not commenting on matters that may or may not be operational;

- Secondly, GCSB and NZSIS do not publicly name foreign states which have, or have attempted to, engage in foreign interference activities. The exception to this is where a deliberate decision is made by the Government of New Zealand to attribute a particular activity to a particular state. This has occurred in relation to selected cyber security campaigns. Such decisions are made with input from a wide range of decision makers.

At the conclusion of this open session, we will be providing a classified briefing to the Committee. This briefing will be at a RESTRICTED national security classification. RESTRICTED information is information which, if publicly released, would be likely to affect New Zealand's national interests in an adverse manner. Our evidence to the closed session will be heard as Parliamentary Secret evidence. This means that our classified information cannot be communicated or used in any form outside of the Committee.

Considerably more information relevant to the Committee's inquiry exists at a higher classification but cannot be disclosed at an UNCLASSIFIED or even RESTRICTED level. This information is, however, communicated to relevant Ministers, the Leader of the Opposition and relevant government agencies. This has occurred over successive administrations.

Our comments in this open session follow the same format as our classified evidence and focus on three main areas:

- How GCSB and NZSIS distinguish foreign interference from legitimate foreign influencing activities;
- Foreign interference threats that GCSB and NZSIS, together with other relevant agencies, considered in the lead up to the 2017 Election and the extent to which they remain relevant today; and
- Security advice that GCSB and NZSIS provide to Members of Parliament and political parties.

Director-General of Security

I will now talk about how we define foreign interference.

Foreign influence v foreign interference

NZSIS and GCSB are mindful of the need to ensure that efforts to prevent foreign interference in New Zealand do not hinder democratically protected rights to political expression, or the ability of states to openly engage and negotiate with each other, including on issues where our perspectives may differ.

NZSIS and GCSB therefore use "foreign interference" only to describe an act by a foreign state, or its proxy, that is intended to influence, disrupt or subvert a New Zealand national interest by covert, deceptive or threatening means.

Interference, so defined, does not include normal diplomatic activities or efforts to garner influence or shape perceptions or policy by open lobbying or persuasion.

NZSIS and GCSB's work prior to the 2017 General Election

Turning now to our work to prepare for the last General Election.

In early 2017 a number of agencies, including NZSIS and GCSB, commenced work looking at vectors for potential interference in New Zealand's General Election. This work, which was additional to our usual and ongoing efforts on a range of foreign interference issues, included:

- First, an intelligence assessment of the threats to the General Election which was informed by the global context at the time, information from New Zealand's security partners, and domestic intelligence holdings;

- Second, GCSB-led work with the Electoral Commission to help protect its core systems and online presence, and to provide advice to parties and candidates in the lead up to the election; and

- Third, an interagency process to develop a protocol that focused on how and when NZSIS and GCSB would engage with other agencies, including the Electoral Commission, if there were a threat to the General Election.

The protocol, which is publicly available on the Department of Prime Minister and Cabinet's website, was not activated.

That the protocol was not activated is no cause for complacency. Interference in New Zealand's elections by a state actor was, and remains, plausible.

Threats to New Zealand's elections and democratic institutions and processes

There are credible reports of interference campaigns in the elections of other countries, and these attempts are increasing in their sophistication.

Last week the Canadian Government released a public document on threats to their democratic processes. That report notes that in 2018, half of all advanced

democracies holding national elections had their democratic process targeted by cyber threat activity. That represents a threefold increase since 2015.

Many states (as well as some non-state actors) retain at least a latent ability to conduct foreign interference activities in New Zealand. A state's decision to do so will be driven by a number of factors:

- Its strategic goals, in particular the value it places on effecting a change in New Zealand's political environment;

- The importance it places on abiding by the norms of international diplomacy;

- Its perception of the effectiveness of the interference activities balanced with the reputational risks of being caught; and

- The importance it places on controlling its diaspora and reducing the space for opposition viewpoints internationally.

Different approaches are preferred by certain foreign interference actors, but we cannot expect approaches to remain static. State actors will use multiple methods to achieve their strategic ends.

The challenge of foreign inference to our democracy is also not just about what occurs around the election itself.

Motivated state actors will work assiduously over many years, including in New Zealand, to covertly garner influence, access and leverage.

I would also note, given public commentary on these issues, that interference efforts do not need to be successful to cause damage to our democracy. Trust in the institutions of government and democracy can easily be eroded.

For these reasons, we must remain constantly vigilant.

The impact of perceived or actual foreign interference in our democracy is potentially serious. For instance:

- Where influence activities are successful, decisions may be made (whether by politicians, voters or policy makers) based on incorrect information;

- Where narratives unpalatable to some foreign governments are repressed, or positive narratives are artificially amplified, the free and open contest of ideas will be constrained. New Zealand's ability to understand, analyse and evaluate certain contentious ideas will be reduced;

- Whether or not interference activities are effective, growing awareness of them creates room for the perception, domestically and internationally, that foreign states wield improper influence in New Zealand. This perception may be concerning to New Zealand's partners and may degrade confidence in our values and democratic institutions; and

- Where a state is able to effectively monitor and influence its diaspora in New Zealand, members of that diaspora – New Zealand citizens and permanent residents – may feel less safe, secure and free in our society.

Vectors for foreign interference in New Zealand's elections

During the classified session, we will brief the Committee on several vectors for foreign state interference in New Zealand's elections. By "vectors", we simply mean the method or channels that a foreign state could use to interfere in New Zealand.

The vectors we will discuss are:

- Cyber-enabled threats to the Election (this encompasses hacking Members of Parliament, candidates and political parties and threats to core electoral systems);

- The use of social and traditional media to spread disinformation;

- Building covert influence and leverage, including through electoral financing; and

- The exertion of pressure or control of diaspora communities.

Within the constraints we have previously outlined, we will be able to provide some information about each of these vectors.

I will now hand-over to Andrew to provide an overview of cyber-enabled threats to New Zealand's Election.

Director General of GCSB

Cyber-enabled interference in New Zealand's elections and democracy

To a large extent, the vulnerabilities of entities involved in New Zealand's elections derive from their function.

For instance, candidates, Members of Parliament and political parties are required to conduct large amounts of external engagement. Their networks must be adaptable and open to accept communication from a wide variety of sources. This presents a large "attack surface" for an adversary.

Individual candidates and political parties also require the lowest level of capability to target; the tools required to do so would be readily available to New Zealand's state-sponsored cyber adversaries and some non-state actors.

At the time of the last General Election, one of the main concerns we had about candidates and political parties being targeted through cyber operations was that information taken would be disclosed with the intent of influencing the election's outcome.

We did not see any activity like this on behalf of a foreign state – but high profile international examples serve as a reminder of the importance of good cyber and information security practices.

This is an area GCSB put significant effort into ahead of the last election.

In the lead up to the election, the National Cyber Security Centre (or NCSC), located in GCSB, assisted the Electoral Commission to provide cyber security advice to political parties and candidates.

Immediately after the election, NZSIS and GCSB provided a protective security brief to incoming Ministers and some other Members of Parliament. These sessions focused on things like the security of their electronic devices and international travel. NCSC remains available to provide support to MPs who have questions about the security of their devices, or their information infrastructure.

There are practical and immediate things MPs – and for that matter, members of the public - can do to protect their cyber security and resilience. Strong passwords, updating security patches, limiting administrator access and "white listing" (allowing only identified users to access a particular privilege) are all important first lines of defence. Human error remains the most common cyber threat vector.

These safeguards will help Members of Parliament, and others, to protect against both state and non-state cyber threats.

Cyber enabled interference in core electoral systems and processes was also an area of focus for the NCSC in 2017. We worked closely with the Electoral Commission on the security and integrity of the Commission's core systems.

The Committee has also asked us to comment on local body elections. I would register GCSB's ongoing concerns about the security implications of proposals to pilot or introduce online voting for local body elections. Manual voting is much less susceptible to compromise and the administrators of local elections do not have the experience or support that the Electoral Commission does, including from my agency.

Disinformation

I would also like to touch briefly on disinformation campaigns. This is an area of growing international interest and concern.

The Canadian report that Rebecca mentioned earlier in her comments noted that cyber interference targeting voters has become the most common type of cyber threat activity to democratic processes worldwide.

Disinformation is false or misleading content that is designed to achieve a strategic purpose. Whether the actor producing and disseminating the disinformation is pursuing ideological or commercial goals, the effort is designed to influence audience perceptions, opinions or behaviour. In the foreign interference context, state actors pursuing their strategic goals through disinformation is an area of focus.

Disinformation can be distinguished from misinformation, which is false or misleading information generally found through the internet, usually placed by private citizens, that is not produced and disseminated in pursuit of an underlying strategic purpose.

It can also be distinguished from malinformation, that is, information that is accurate, but acquired and/or released in a way that it is intended to discredit an individual or group. Email or data hacks and subsequent leaks are an example of malinformation.

Disinformation and malinformation are not new phenomena. They can be, and have been, spread by blogs and 'news' websites, and more traditional forms of media such as leaflet drops. However, their potential impacts have been amplified in recent years by a number of factors including:

- The exploitation of cyberspace – its free and open nature, and its ability to distribute content widely and quickly;

- The automation of content creation and distribution (including using artificial intelligence methods);

- The increasing use of 'clickbait' news websites and social media platforms; and

- The increased intent and capability of state actors to use disinformation and malinformation to influence domestic or foreign politics in pursuit of their strategic goals.

To date, New Zealand has not been the direct target of widespread state-backed disinformation or mal-information campaigns.

But members of the New Zealand public are highly likely to encounter them, such is the international nature of online content. This means that disinformation campaigns occurring overseas may affect levels of trust in media and government here. This would most likely impact on domestic debates fuelled by distrust of authority and facts.

The role of intelligence and security agencies in responding to disinformation, or "fake news" and social media manipulation is potentially very fraught as it could be perceived as interference in political debate, individuals' freedom of expression or privacy.

Our agencies' role is therefore limited in this area and conservative. We do not have the legal authority, technical means, or indeed the social licence to monitor all of the country's internet activity. However, if we receive reporting from security partners, political parties or the public, that suggests a state sponsored disinformation or malinformation attack is afoot, we would assess it for further investigation.

I will now hand back to Rebecca to talk about the last two vectors,

- The exertion of pressure or control of diaspora communities; and

- Building covert influence and leverage, including through electoral financing.

Director-General of Security

Diaspora communities

Manipulation of expatriate communities is a vector for interference. Some states engage overtly or covertly with their diaspora as a means to achieve strategic aims. NZSIS is aware of efforts by foreign states to covertly monitor or obtain influence over expatriate communities in New Zealand. Shared culture, language or familial connections can facilitate this. Ongoing family ties in the

foreign state can be leveraged to suppress unwelcome political or religious activity.

Foreign language media is another way through which expatriate communities or diaspora populations can be influenced or mobilised towards particular issues, including issues relevant to elections.

Using relationships and donations to influence and leverage

Moving now to covert influence and leverage, including political donations.

NZSIS's starting point in this area is that relationship building is a normal, legitimate and expected part of the way other states' operate in New Zealand. NZSIS is only concerned where an aspect of the relationship verges on or actually constitutes foreign interference. I touched on the definition of foreign interference earlier in my remarks.

Similarly, political donations are a legally sanctioned form of participation in New Zealand politics. However, NZSIS becomes concerned when some aspect of the donation is obscured or is channelled in a way that prevents scrutiny of the origin of the donation.

One of the main reasons we become concerned about these activities is because as relationships of influence, or a sense of reciprocity is established, they may be used as leverage to facilitate future interference or espionage activity.

I have already commented on the constraints we face in talking about specific intelligence. However, in broad terms, I can say that we have seen activities by state actors that concern us.

I can also say that motivated state actors are adept at finding weaknesses or "grey areas" to help them to covertly build and project influence. Total transparency of the regulatory regimes governing our elections and democracy is the best counter to this.

We also need to equip those on the front line of our democracy - Members of Parliament, Ministers, political parties and relevant government agencies - with the capability to identify and protect themselves from foreign interference risks. NZSIS and GCSB do this through our outward-facing security

functions (the Protective Security Requirements Team and the National Cyber Security Centre).

We consider there is more we can do to systematise the protective security support we currently provide to Members of Parliament, Ministers and people working in the Parliamentary Complex. To that end, I intend to write to all party leaders offering protective security briefings to Members of Parliament.

My agency, and the GCSB, are available to speak with any Member of Parliament who has concerns about foreign interference in our democracy or elections, or about their own personal protective security practices.

Director General of GCSB

I would like to close by noting that the refreshed National Security and Intelligence Priorities, which are set by Government, will ensure that the New Zealand Intelligence Community is well coordinated, and working alongside other relevant government agencies, to address threats to New Zealand's next election.

Given the high interest in this issue, we seek the Committee's permission to publicly release this statement immediately.

We are happy to answer your questions.